普通高等教育“十三五”规划教材

安全科学与工程系列

第3版

安全系统工程

主编　张景林

煤炭工业出版社

普通高等教育“十三五”规划教材

安全系统工程

（第3版）

主编　张景林

煤炭工业出版社

·北　京·

内 容 提 要

本书是普通高等教育“十三五”规划教材（高等院校安全工程专业）之一。本次修订在大的章节内容上保留了原教材的格局，但是具体内容上作了若干修改，如第二章的事故隐患和危险性分析及第四章的系统安全评价方法；增加了安全预测和典型事故模型分析的内容等。本书全面地介绍了安全系统的概念、事故隐患和危险性分析、事件树和事故树分析、系统安全评价、系统安全预测和安全决策、安全系统建模与典型事故影响模型。

本书主要作为高等院校安全工程专业学生教材，也可供安全工作者参考。

序

安全是人类生存、生产、生活和发展过程中永恒的主题。随着科技与经济的迅猛发展，安全科学的日臻完善，安全工程专业已经成为高校重点专业之一。为此，高等院校安全工程专业教育指导委员会在全体委员对课程设置、教学大纲等进行充分论证的基础上，组织编写了《安全学原理》《安全系统工程》《安全人机工程学》和《安全管理学》四门安全工程专业的专业基础课教材。经各编写组认真编写，主审人审查，高等院校安全工程专业教学指导委员会审定，现组织出版并作为高等院校安全工程专业本科推荐教材。

高等院校安全工程专业教学指导委员会

2002 年 4 月

第 3 版修订说明

《安全系统工程》自 2014 年初第 2 次修订出版后，依然得到了广大师生的一致好评。但随着时代的发展，安全系统工程理论、方法和技术得到了快速发展，有些内容已不适应需要。为了使《安全系统工程》更适应社会和专业发展的需要，更好地为广大从事安全学习与工作的读者服务，我们在第 2 版的基础上进行第 3 次修订。

本次修订，在保持原有内容的基础上，结合近年来我国安全工程学科领域的研究和实践，对部分知识的相关内容、方法、案例等方面进行了相应的补充和更新。一是针对网络安全、人工智能系统等的风险、安全评价、失误率提出方法补充（第二章和第五章均有详细介绍）；二是更加全面、系统地介绍了事故隐患和危险性分析（第二章内容）和系统安全评价方法（第四章内容）；三是增加了安全预测和典型事故模型分析的内容，并对二次修订的某些释义、案例、引用的标准、规范结合近几年学科的发展进行再一次的审视和修正。这些修订力求能够全面反映当前安全系统工程的先进理论、理念和方法，以典型应用实例和模型指导学生更好地将理论知识应用于实践。

本次修订工作由中北大学张景林负责全书的统稿，并负责第一章的编写，第二、三章由吕春玲编写，第四、五、六章由杨继华编写。由北京理工大学汪佩兰教授担任主审。

本次修订工作得到了中北大学和北京理工大学相关领导和老师的指导和帮助，在此向他们表示衷心感谢。

由于编者水平有限，本书中可能存在不足之处，真诚希望得到读者的批评和指正。

编　者

2018 年 6 月

前　言

本教材是安全工程专业必修专业基础课，其先修课程为概率统计、线性代数、安全学、系统工程学和计算机应用技术等。

本教材在选材上力求新颖，尽量吸取近年来的教学实践和国内外最新科研成果；体系上注意完整性、条理性，并从安全科学学科发展的高度，充实和完善其内容；对难点，将通过由感性到理性，从现象到本质的方法，用通俗形象的语言来阐述，并且注意给出尽量多的例题，以便于学生理解和自学，有利于培养学生分析问题和解决问题的能力。本教材教学时数为48学时，每章后均有思考题，供学生思考和练习。

本书编写工作是在高等院校安全工程专业教学指导委员会的直接领导下进行的，从教材大纲的编制、审定及其与相关教材内容的划定，均由安全工程专业教学指导委员会反复讨论完成。作者严格遵照大纲的规定与要求，结合近年来的教学实践与研究工作，编写了这本《安全系统工程》教材。全书共分六章，包括：概论、系统安全分析、事故树分析、系统安全评价、安全决策和灰色理论与安全系统。其中，第一章由崔国璋、张景林教授编写，第二章由王福成教授编写，第三章由赵艳萍编写，第四、五章由张景林教授编写，第六章由赵云胜编写。全书由张景林、崔国璋教授统稿，北京理工大学汪佩兰教授担任主审。汪佩兰教授对本教材进行了全面、认真、严格、细致的审查，提出了许多宝贵的修改意见。王建华、柴涛、吕春玲老师对书稿的校正、打印、完善作了许多具体工作，在此向她们表示诚挚的谢意。本书还引用了大量的文献资料，涉及许多中外学者，在此一并向他们表示感谢。

编　者

2001年12月

第一章 绪 论

“安全系统工程”是“安全科学与技术”一级学科下的二级学科。“安全系统工程”是以研究大规模复杂系统为对象的一门新兴的学科。它把自然科学和社会科学有关的思想、理论和方法，根据系统总体协调的需要有机地联系起来，识别、排查、分析和评价系统中存在的事故隐患及危险性，从而作出危险性预测和系统安全决策。

人类社会发展日新月异，特别是军事、信息网络、材料等方面不断取得新的突破和创新，不断刷新人们的传统认识和科学观念。但是不管社会、科学如何发展，安全问题仍然是人类社会生存、生产、生活的首要命题。

虽然社会各个领域的安全问题各有特殊性，但是，一方面应该看到各个领域安全问题既有区别又有联系，相互影响；另一方面也应该从大安全角度出发，总结提升它们的共同点，寻求各个领域安全问题内在的共同规律和联系。这也正是安全系统研究发展的重要内涵和目的。

第一节 系统工程的概念

一、系统和系统工程

1. 系统

系统就是由相互作用和相互依赖的若干组分结合而成的具有特定功能的有机整体。

系统有如下特点：

（1）整体性。系统是由两个或两个以上相互区别，同时又具有相关性的要素（元件或子系统）组成的整体。构成系统的各个要素虽然具有不同性能，但它们通过综合、统一（不是简单拼凑）形成的整体就是具备了新的特定功能，就是说，系统作为一个整体才能发挥其应有的功能。所以，系统的观点是一种整体的观点，一种把部分整合在一起的思想方法。

（2）相关性。构成系统的各要素之间、要素与子系统之间、系统与环境之间都存在着相互联系、相互依赖、相互作用的特殊关系，通过这些关系，使系统有机地联系在一起，发挥其特定功能。

（3）目的性。任何系统都是为了完成某种任务或实现某种目的而发挥其特定功能的。要达到系统的既定目标，就必须赋予系统规定的功能，这就需要在系统的整个生命周期，即系统的规划、设计、试验、制造和使用阶段等，对系统采取最优规划、最优设计、最优控制、最优管理等优化措施。

（4）有序性。系统的有序性主要表现在系统空间结构的层次性和系统发展的时序性。系统可分成若干子系统，子系统下面还能分出更小的子系统，这种系统的分割形式表现为系统空间结构的层次性。另外，系统同样是有寿命周期的，它也要经历孕育、诞生、成

长、成熟、衰老、消亡的过程，这一过程表现为系统发展的有序性。对系统进行分析、评价、管理都应考虑系统的有序性。

（5）环境适应性。系统是由若干特定部分组成的有机体，处在这个有机体以外的部分，通常称为系统的环境。一方面，系统需要从环境中获取必要的物质、能量和信息，同时系统对环境也要进行反馈；另一方面，当环境对系统产生干扰和限制时，即为环境对系统的约束条件。环境特性的变化往往能够引起系统特性的变化。系统要实现预定的目标或功能，必须能够适应外部环境的变化。

应该看到，能够满足上述特点的称得上是系统的客体，是多种多样的。例如，自然系统与人造系统、封闭系统与开放系统、静态系统与动态系统、实体系统与概念系统、宏观系统与微观系统、软件系统与硬件系统等。

2. 系统工程

系统工程是组织管理系统的规划、设计、制造、试验和使用的科学方法，是一种对所有系统都具有普遍意义的科学方法。这个定义的内涵是：系统工程属于工程技术范畴，是组织管理各类工程的方法结论；系统工程是解决系统整体及其全过程优化问题的工程技术。

系统工程是20世纪50年代发展起来的一门新兴科学，它是以系统为研究对象，以现代科学技术为研究手段，以系统目标最佳化为研究目的的科学技术。它属于管理科学，它的广泛应用为各行各业、各个领域实现管理现代化提供了基本理论和方法。

关于系统工程所属各自学科的命名问题，钱学森教授指出：正如工程技术各有关专业一样，系统工程也还是一个总类名称，因体系性质不同，还可以再分类，如工程体系的系统工程叫某某工程系统工程（如人工智能系统工程），生产企业或企业体系的系统工程叫经济系统工程等。这种命名原则为系统工程在各专门领域的发展指明了方向，从而也避免了关于名词术语叫法的不必要的争论。

二、可靠性和可靠性工程

1. 可靠性

可靠性是指系统在规定条件下和规定时间内完成规定功能的能力。这里，规定的条件是设计规定的，规定的功能也是设计赋予的。衡量系统可靠性的最低指标是可靠度，它是用系统在规定时间内完成规定功能的概率来表示。相反，系统在规定的条件下和规定的时间内不能完成规定功能的概率就是系统的不可靠度。

2. 可靠性工程

可靠性工程就是研究系统可靠性的工程技术。可靠性工程就是要解决如何提高系统的可靠度，使系统在其寿命周期内正常运行，圆满完成其规定任务。

在某些产品的经典设计中，例如一些机械结构承压件，其安全系统被定义为强度均值与应力均值之比，此时产品的可靠度则被称为安全系数大于1的概率。对于一个系统而言，系统的可靠性与系统的安全性是两个既有区别又紧密联系的功能。当一个系统的功能运行可靠度不好时，其系统的安全性必然会受到质疑；同样，一个安全性不好的系统，它也不能可靠运行。

三、安全系统与安全系统工程

1. 对安全的理解和认识

安全一词是人们经过抽象思维确定的一个概念或理念。目前所见到的文献对安全一词诠释普遍存在两个问题：一是缺乏科学的严密性，比如说只要不出事故就是安全的，显然这是不严密的说法，因为事故是不安全因素发展的极端表现；二是安全一词应用得太宽泛，不管人们如何定义都很难包容各种情况下的安全的内涵。

安全描述的是一种客观存在的状态吗？回答并非是肯定的，因为描述安全状态的主要特征量是什么，在安全科学界尚难统一。有人说，无事故且无隐患的状态才是安全状态；也有人提出用系统从无序到有序、渐变与突变的统一及非畸变来描述安全的动态特性。这样的表述虽然有一定的科学性，但由于安全因素的高度复杂性和极强的时间依赖性，上述方法所描述的安全状态带有很大的理想化色彩。但是，人们很难把握实际的安全状态究竟是处于“平安无事”，还是处于危险的某个阶段；此外，人们所说的平安、安全是人们的一种带有理念性的一种期盼，此时安全不过是一种理想化的抽象概念。

如果承认“安全”一词描述的是一种状态，但这种状态也绝非是一种事故为零的所谓“绝对安全”的状况。从科学的角度讲，“绝对安全”的状态在客观上是不存在的。平安也好，安全也好，其本身就带有很大的模糊性、不确定性和相对性，所以“安全状态”具有动态特征，就是说，与一般“状态”概念不同，安全状态的动态特性说明了“安全状态”的表征的特殊性。

安全的动态特征还体现在安全描述的不只是相对稳定的特定状态，同时安全还可以作为过程表征，用来描述事故——相对安全的一个阶段。过程表征和状态表征最本质的区别就在于前者描述的是事物的发展趋势，后者描述的是一种目标。从这个角度讲，把安全状态和安全过程看成是一个事物的两个方面，它们没有办法严格区分开来。正如有的文献所描述的：渐变对应于灾害过程孕育、维持；突变对应于灾害过程的活动和剧烈的扩展。但是，突变（事故）不仅是灾害发生，也是系统内不稳定向新的稳定（安全）跃迁的触发器。

当然从技术的角度讲，已经提出并应用的安全失效率、安全度、安全系数等定量化的并涉及安全的计算方法标准及表征的安全技术状态和安全与否的结论是科学严谨的。但是，这和上面讨论的安全内涵相比显然要狭义得多。

状态、过程、理念、技术安全都是定义安全这个概念应该考虑的内涵。因此，人们试图通过一个简单的定义就想把内容如此丰富、关系如此复杂、时空跨度难以界定的若干事物表述清楚是一件非常困难的事情。

从科学的原理出发，定义事物多采用两种方法：一种是从事物的组成考虑；另一种是从事物的功能考虑或两者兼顾。依据上述分析，我们对安全定义如下：安全表述的是一个复杂系统的动态过程或一个特定的相对稳定的状态，过程或状态的目标在受时间和风险大小约束的条件下，使人、物不会受到伤害或损害。安全也可表述为人们的一种理念，即没有危险，不存在隐患，不出事故的理想状态。

2. 安全的属性

安全所涉及的因素是纷繁的，因素之间以及因素与目标之间的关系是复杂的，这些都

与安全的属性有关。这里讨论的安全属性主要是指人的安全，因为人的安全永远是讨论安全问题的主命题。

1）安全的自然属性

安全的自然属性可以从主动和被动两个方面来描述。

（1）安全是人的生理与心理需要，或者说由生命及生的欲望决定了的自我保护意识，这是天生的，是安全存在的主动因素。

（2）人类对天灾的无奈以及新陈代谢、生老病死的规律不可抗拒，使人们不得不把生命安全经常提到议事日程，这虽然是被动因素，但它与前一个主动因素相结合，就决定安全是自古以来人类生活、生存、进步的永恒主题。

2）安全的社会属性

安全的社会属性也可以从主动和被动两个方面来表述。

（1）自从人类有组织活动以来，社会安定、有序、进步始终是各社会阶段追求的目标，而这一目标实现的重要标志之一就是安全，因此这是安全立足社会的主动因素。

（2）人类的社会活动如政治的、军事的、文化的等，有的对安全直接起破坏作用，有的间接影响着安全；人类的经济活动如生产（职业）、高技术灾害（化学品致灾、核事故隐患、电磁环境公害、航天事故、航空事故）、交通灾害则是自人类开展经济活动以来就存在的突出的安全问题；如今更加突出的一个安全问题是环境问题，环境恶化（包括自然环境和人为环境）是人类生活、生存安全的重要威胁。例如，在15届世界职业安全卫生大会上，与会专家指出：向21世纪人们提出的挑战性问题是“环境、安全、健康问题”，即Q. E. &OSH是一个严重影响国民经济可持续发展的大问题。显然，由于社会科技的发展带来或产生的安全问题反过来影响了或阻滞了社会的发展，才使安全问题的解决提上议程，这就是安全社会属性的被动性。

可以看出，安全的自然属性与社会属性中都存在着促动安全的主动因素，这正是安全科学发展的客观基础。

安全问题纷繁复杂的关系正是由于安全问题的自然属性与社会属性的交融，正像人是社会属性一样，社会的复杂性使人际关系复杂，社会的复杂性也是安全问题复杂的重要原因之一。

3. 安全系统及其特点

安全问题是一个复杂的系统工程问题。或者说，解决安全问题要用系统工程的理论和方法。这就是说为了科学地规划、解决安全问题，首先要把与安全相关的若干因素构建成安全系统，并确定因素之间的相互关系和系统目标。

安全系统，区别于其他系统构建的关键在于要掌握其特殊性和客观性。所谓特殊性就是指它与一般系统的区别；所谓客观性就是要分析给出安全系统与一般工程系统的关系。安全系统是能够完成预定功能的大的工程系统的子系统，也是安全系统自成体系。

安全系统的特点可以归纳为以下5个方面。

1）系统性

与安全有关的影响因素构成了安全系统。因为与安全有关的因素纷繁交错，所以安全系统是一个复杂的巨系统。一方面，安全系统所涉及的因素数量及相关性复杂程度都明显高于一般系统；另一方面，安全系统各因素之间以及因素与目标之间的关系多数有一定灰

度，所以安全系统是灰色系统。

与一般系统不同，安全系统把环境因素看成是系统的组成部分。安全系统典型的组成因素及其关系如图 1-1 所示。

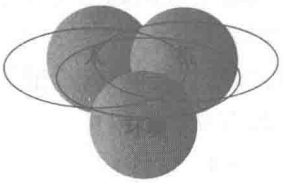

图 1-1　安全系统典型的组成因素及其关系图

依据安全问题所涉及范围大小不同，安全系统大小之差可能很悬殊。一般地讲，纯属技术领域的安全系统比如一台设备、一辆无人驾驶的机动车，可能只涉及机和物；而对于一个车间、一个工厂，要考虑其安全系统，则不只是机和物，肯定还要考虑人、环境等因素。实际上，人—机—环境的提法是考虑了安全问题的空间跨度和时间跨度两个方面。如此说来，即便只是一台设备，如果把它的制造、运输、安装、使用过程中安全问题都考虑到，也仍然是一个“人—机—环境”的复杂系统。

安全系统的目标不是寻求最优解。这是因为安全系统目标的多元化，以及安全目标的极强相对性、时间倚赖性及与其理想化理念很难协调，所以安全系统的目标解是具有一定灰度的满意解或可接受解。

2）开放性

安全系统是客观存在的。这是因为安全系统的功能构件是物质的，但同时安全系统多是寄生在客体（另一个系统）中。在处理方法上，如果把客体看成一个黑匣子，安全系统则是通过客体的能量流、物流和信息流的流入—流出的非线性变化趋势，确认安全和事故发生的概率，因此安全系统具有开放性特点。

开放性不仅是安全系统在动态中保持稳定存在的前提，也是安全系统复杂性及安全—事故转换发生的重要机制。

3）确定性与非确定性

确定性是指制约系统演化的规则是确定性的，不含任何随机性因素。确定性的特征是演化方向及演化结果是确定的，可精确预测。

非确定性或者具有演化方向和演化结果的不确定性特征，或者具有刻画事物运动特征的特征量不能客观精确地确定。非确定性包括随机性和模糊性。

随机性可能有两个方面的来源：一是在不含任何外在的随机影响因素作用下，完全由确定性系统演化而产生的随机性（例如产生混沌），这种随机性称为本质随机性；二是系统还可能因其外在影响因素的随机作用而产生随机性行为，从而使系统在一定条件下表现出随机性的特征，这种随机性称为外在随机性。由于安全系统把环境看成是它的组分，所以对安全系统而言，本质随机性和外在随机性的区别不是绝对的。

模糊性是指事物的本身不清楚或衡量事物的尺度不清楚。对于安全系统，就是指系统的构成及其相互关系，以及组成与目标的关系不清楚。造成这些不清楚的可能来源在于主观和客观两个方面，即具有主观模糊性和客观模糊性。首先，刻画安全运行轨迹的以模糊

数学方法建立的数学模型具有主观模糊性。因为数学模型常常不可能“严格地”确定安全系统各要素之间及其与目标之间完整的客观关系。当然，对于自然的技术因素之间的关系尚好一些。而对于社会的因素及其与技术因素的耦合关系将难于量化，因而也将难于建立准确的数学关系。应该强调的是，出现上述问题不完全是由于安全系统本身不清楚，它可能只是人们对安全系统主观模糊性的表现。

另外对安全系统安全度的评价尺度以及构成安全度等级的评价指标体系也具有客观模糊性，即从事物的本质上无法给出其客观衡量尺度。

4）安全系统是有序与无序的统一体

序主要反映事物的组成规律和时域。依据序的性质，可分为有序、混沌序和无序。有序通常同稳定性、规则性相关联，主要表现为空间有序、时间有序和结构有序。无序通常与不稳定、无规则相关联。而混沌序则是不具备严格周期和对称性的有序态。现代复杂系统演化理论认为，复杂系统的演化中，不同性质的序之间可以相互转化。安全系统序的转化结果是否引发灾害或使灾害扩大，取决于序结构的类型及系统对特定序结构下运动的（灾害意义上的）承受能力。

有序和无序，确定性和非确定性都会在系统演化过程中通过其空间结构、时间结构、功能结构和信息结构的改变体现出来。

5）突变性或畸变性

安全系统过程的突变或畸变，或过程由连续到非连续变化在本质上是服从于量变引起质变的哲理。

量变到质变的转化形式可以用畸变、突变或飞跃来描述，但也可通过渐变实现。所以安全系统的渐变也可能孕育着事故，而突变、畸变则肯定对应于灾害事故的启动，是致灾物质，或能量的突然释放。

综上所述，安全系统虽然与一般系统、非线性系统等有若干共同点，但安全系统的个性还是非常明显的，这是决定它客观存在并区别于其他系统的根本原因。

4. 安全的动力学特征

安全系统是物质系统。安全过程既可能是自组织的，也可能是被组织的，也可能两者兼而有之。

所谓自组织的，是指系统在获得空间、时间或功能的结构过程中，没有外界的特定干预（所谓外界的特定干预，对安全来说主要是指社会属性中的被动因素）。它可能有两种发展形式：一种是非组织的向组织的有序发展过程，其本质是组织程度从相对较低到相对较高演化；另一种则是维持相同组织层次，但复杂性相对增长。前一种过程反映了安全系统组织层次跃升过程，而后一种过程则标志着安全系统组织结构与功能从简单到复杂的组织水平的提高。

对安全系统自组织的演化过程主要是反映它的自然属性与社会属性共同作用的过程和结果。因为安全系统是开放系统，它可以不断与外界交换物质、能量和信息，从而出现上述的两种发展形式，即从原有的混沌无序状态，转变为一种在时间、空间或功能上的有序状态。

一旦安全过程出现被组织的情况：如不可预见的天灾、人为诱发地震、战争、人为纵火、违规操作等，则会发生灾难或事故。

当然安全系统也是非线性系统，因而也具有非线性系统的共同特征。非线性是系统产生自组织行为的内因，没有这个内因，所谓开放性将不起作用，无序—有序的过程也就不会发生。

不少学者提出并论证了安全系统是以耗散结构形式存在的，这种耗散结构通过自组织形成并维持下去。而耗散结构最本质的特性就是消耗外界有序的物质、能量和信息，没有消耗，耗散结构将不复存在。因此，要维持安全系统的耗散结构，必须保证安全系统的开放性，使得物质、能量和信息的流入与流出达到平衡。据此，引进“负熵流”和“正熵流”的概念以从定性角度来考虑安全系统与外界的物质能量和信息交换；引进“剩余熵”的概念以从定量角度来获得体系失稳与否的判据。虽然都有一定的局限性，但熵仍然是今后研究安全过程发展趋势的重要概念和方法。因为熵的大小是状态自发实现可能性的量度，熵的变化量能反映出安全系统混乱度的变化情况，其具有以下数学关系：

$$\Delta \text{剩余熵} = \Delta \text{熵增} - \Delta \text{负熵流} - \Delta \text{正熵流}$$

如果 Δ 剩余熵为正数，则表示安全系统混乱度的增加；如果 Δ 剩余熵为负数，则表示安全系统的有序度的增加；如果 Δ 剩余熵为零，则表示安全系统处于稳定状态。所以，安全系统耗散结构的维持，Δ 剩余熵不能为正数。

那么，安全系统的熵如何表达呢？描述某一个零部件，在特定条件下，完成其特定功能的能力，一般用可靠性来表示。同样，对于一个安全因素 x_i，可以用其安全度 $P(x_i)$ 来表示在某一等级的耗散结构下，完成其规定的安全功能的能力。而安全度的大小，又可以从熵的角度来分析，它必然有一个与安全度相对应的安全熵来表示该安全因素的不确定度、混乱度和无序度。当安全度越大时，安全因素的不确定度、混乱度和无序度就越小；反之，其混乱度也就越大。

从熵的本质含义出发，熵是系统状态概率 ω 的量度 S，即 $S=k\ln\omega$。在参考信息熵的定义之后，提出安全熵的概念及其定义。安全熵是安全因素自身状态混乱度的一种量度，用安全度 $P(x_i)$ 来定义其安全熵为

$$S(x_i) = k\log\frac{1}{P(x_i)} = -k\log P(x_i) \quad (i = 1, 2, \cdots, n)$$

其中，k 为待定系数，所谓的待定系数是为了与其他理论方面相结合而起到桥梁作用，设 $k=1$，安全熵的表达式简化为

$$S(x_i) = \log\frac{1}{P(x_i)} = -\log P(x_i) \quad (i = 1, 2, \cdots, n)$$

上述的这一公式说明，当安全度 $P(x_i)$ 越大时，对应的安全熵 $S(x_i)$ 就越小，特别是当 $P(x_i)=1$ 时，对应的安全熵达到最小，$S(x_i)=0$，这时认为该安全因素混乱度为零，与实际情况相吻合。同理，当安全度 $P(x_i)$ 越小时，对应的安全熵 $S(x_i)$ 就越大，说明该安全因素混乱度越大，执行该安全功能的能力就越差。

在这里特别说明的是，安全熵是严格利用安全因素本身的安全度来进行定义的，即利用的是安全因素完成其安全功能的状态概率。安全因素的状态概率是统计数据，某个安全因素在某些情况（状态）下存在的概率，需要积累数据，同时对其状态的判定也需要有一定的依据。

5. 安全系统工程

安全系统工程是采用系统工程的基本原理和方法，预先识别、分析系统存在的危险因素，评价并控制系统风险，使系统安全性达到预期目标的工程技术。安全系统工程是从根本上和整体上来考虑安全问题的，它为安全工作者提供一个既能对系统发生事故的可能性进行预测，又可对安全性进行定性、定量评价的方法，从而为有关决策人员采取安全措施提供决策依据。

对安全系统工程的定义，还可以从以下几个方面进行理解：

（1）安全系统工程的理论基础是安全科学和系统科学。它是以工矿企业、交通运输、劳动安全卫生领域为主要对象的一门工程技术。

（2）安全系统工程的重点内容是系统危险因素的识别和分析、系统风险评价、系统事故控制和系统安全决策。

（3）安全系统工程要达到的预期安全目标是系统风险控制在人们能够容忍的限度以内，也就是在现有经济技术条件下，最经济、最有效地消除事故隐患，降低事故发生的概率。

（4）安全系统工程对风险的控制是动态的，不只是目标风险控制，也包括过程风险控制。

第二节　安全系统工程的研究对象、研究内容及方法

一、安全系统工程的研究对象

安全系统工程作为一门科学技术，有它自身的研究对象。任何一个生产系统都可以概括为3个部分，即从事生产活动的操作人员和管理人员，生产必需的机器设备、厂房、原材料、成品或半成品以及生产活动所处的环境。这3个部分构成一个“人—机—环境”系统，每一部分就是该系统的一个子系统，称为人子系统、机器子系统和环境子系统。

1. 人子系统

该子系统的安全与否涉及人的生理和心理因素，涉及规章制度、规程标准、管理方法、措施是否适合体现以人为本的理念，是否易于为人们所接受。研究人子系统时，不仅把人当做“生物人”“经纪人”，更要注意人的社会属性，必须从社会学、人类学、心理学、行为科学角度分析并解决问题；区别于其他子系统，要看到人是一种自尊自爱、有感情、有思想、有主观能动性的生物。在人工智能系统中，疲劳失误和反应速度上人是比不过机器人的，但在应激判断上机器人又存在局限性。这些都有待于人子系统内涵的进一步拓展。

2. 机器子系统

对于该子系统，一方面是设备的运行可靠性和安全装置、安全设施的有效性，而且要考虑设备仪表、操作性等是否符合人机工程设计要求；另一方面要考虑加工所涉及的原材料、半成品、成品的工艺安全性以及对人的心理和生理安全可能带来的影响等。

3. 环境子系统

一般环境子系统应该包括凡是与安全系统产生能量、信息、物质交流所波及的范围

(时空) 都属于环境子系统。

对于该子系统，主要考虑系统与环境之间交流产生的与安全有关的理化因素和社会因素影响。理化因素主要有噪声、振动、粉尘、有毒气体、射线、光、温度、湿度、压力、热、化学有害物质等；社会因素有管理制度、经济效益、社会安定、人际关系等。

3 个子系统相互影响、相互作用的结果使系统总体安全性处于某种状态。例如，某些理化因素影响机器的寿命、精度，甚至最终导致机器的损坏；某些机器产生的噪声、振动、温度、尘毒又影响人和环境；人的心理状态、生理状况往往是引起误操作的主观因素；环境的某些波动又会影响人的心理状态，给安全带来潜在的隐患。这就是说，这 3 个相互联系、相互制约、相互影响的子系统构成了一个“人—机—环境”系统的有机整体。分析、评价、控制“人—机—环境”系统的安全性，只有从 3 个子系统内部及 3 个子系统之间的这些关系出发，才能合理解决系统的安全问题。

二、安全系统工程的研究内容

安全系统工程是专门研究如何用系统工程的原理和方法确保实现系统安全功能的科学技术。其主要技术方法有事故隐患和危险性分析、系统安全评价和安全决策与事故控制。

1. 事故隐患和危险性分析

要提高系统的安全性，使其不发生或少发生事故，其前提条件就是预先发现系统可能存在的危险因素，全面掌握其基本特点，明确其对系统安全性影响的程度。只有这样，才有可能抓住系统可能存在的主要危险，采取有效安全防护措施，改善系统安全状况。这里所强调的“预先”是指：无论系统生命过程处于哪个阶段，都要在该阶段开始之前进行系统的安全分析，发现并掌握系统存在的事故隐患。这就是事故隐患和危险性分析要解决的问题。

事故隐患和危险性分析是使用系统工程的原理和方法，辨别、分析系统存在的危险因素，并根据实际需要对其进行定性、定量的分析和表征。

事故隐患和危险性分析已有比较多的方法和形式，应用时应该注意以下几点：

(1) 根据系统的特点、分析的要求和目的，可采取不同的分析方法。因为每种方法都有其自身的特点和局限性，并非每种方法都通用。使用时要综合应用多种方法，对结果进行比较验证，从而得出更加满意的结果和结论。

(2) 使用现有的分析方法不能死搬硬套，必要时可根据实际情况进行方法修正和结论修订，但要有充分的修改依据。

(3) 不能局限于现有分析方法的应用，一方面，原有方法不应该是一成不变的；另一方面，新技术、新概念的事物不断涌现，新的危险因素出现必然要有新的认识和分析方法与之相适应。

2. 系统安全评价

系统安全评价往往要以事故隐患和危险性分析为基础，然后通过安全评价分析了解和掌握系统存在的危险因素，但不一定要对所有危险因素采取措施。而是通过评价掌握系统的事故风险大小，据此与系统安全指标或安全标准相比较，如果超出指标，则应对系统的主要危险因素采取控制措施，使其降至该标准以下。这就是系统安全评价的任务。

安全评价方法有很多种，应根据评价对象的特点、规模，评价的要求和目的，采用不

同的方法。同时，在使用过程中也应和事故隐患、危险性分析方法的使用要求一样，坚持实用和创新的原则。

我国开展安全评价已有 20 多年的历史。现在一方面，已有专门机构从事安全工作；另一方面，凡是重大工程项目，特别是一些高危作业，工程从立项、设计开始，必须进行安全评价。这就体现了安全工作在生产领域占有重要的地位。

3. 安全决策与事故控制

事故隐患和危险性分析以及安全评价是解决安全问题的第一步，在此基础上才能进行系统安全决策。系统安全决策是从系统的完整性、相关性、有序性出发，对系统存在的安全问题实施全面、全过程的安全技术管理，以实现系统安全目标的控制。目前，有关的安全系统目标与控制在很多领域已形成标准，如美军标准《系统安全程序》，美国道化学公司的《安全评价程序》，国际劳工组织、国际标准化组织倡导的《职业安全卫生管理体系》等。

三、安全系统工程的方法

由于实际的社会生产安全系统目标的多样性，若要实现这些目标，就得使相应的安全系统工程方法产生多元化，但是这些方法均是依据安全科学理论，在总结过去经验型安全方法的基础上，逐渐丰富和成熟起来的。

1. 从系统整体出发的研究方法

安全系统工程的研究方法必须从系统的整体性观点出发，从系统的整体考虑解决安全问题的方法、过程和要达到的目标。例如，对每个子系统安全性的要求，要与实现整个系统的安全功能和其他功能的要求相符合。在系统研究过程中，子系统和系统之间的矛盾以及子系统与子系统之间的矛盾，都要采用系统优化方法寻求各方面均可接受的满意解。同时，要把安全系统工程的优化思路贯穿到系统的规划、设计、研制和使用等各个阶段中。

2. 本质安全方法

有人把本质安全说成是绝对安全，这种说法是不全面的。其实本质安全说的是从技术角度将凡是人能想到的不安全因素都已解决或有相应的安全技术措施，从而使机（物）达到本质安全的状态。当然，对于本质安全也有人提出不同的解释。黄槐在《本质安全别解》中提出：一是认为真正的本质安全是在寻求人的安全的高可靠性、也就是人的行为的零失误；二是认为企业即使在技术上和经济上有了巨大的投入，在机器、设备、装置方面实现了本质安全，如果没有一批高素质的人，也未必能使技术设备等方面的优势形成真正的本质安全；三是真正过程的本质安全是通过人的安全行为来实现的。把人的安全意识提高到自觉或自律的水平，并在此基础上加强严格的安全管理，实施“人本管理”，所以“本质安全”是实现安全过程和安全目标的关键，不仅具有相对性，而且只有在科学技术与经济基础发展到一定水平和高度的条件下才能真正实现；还应当把人的因素提高到人是保证安全的主导因素的高度来对待，因为人具有应变能力，在安全管理中要把“人本”和“人本管理”作为实现“本质安全”的指导思想和重要手段。

本质安全方法是安全系统工程方法中的核心内容，安全系统工程就是研究实现系统本质安全的方法和途径。

3. 人—机匹配法

随着科学技术的进步，虽然人类的生产劳动越来越多地为各种机器（机器人、无人驾驶飞机、汽车等）所代替，但人在影响系统安全的各种因素中，至关重要的还是因为系统不能完全脱离人的参与、干预、判定，这就是所谓的人—机匹配。在产业部门研究与安全有关的人机匹配，称为安全人机工程；在人类生存领域研究与安全有关的人机匹配，称为生态环境和人文环境问题。显然从安全的目标出发，考虑人—机匹配以及采用人—机匹配的理论和方法是安全系统工程方法的重要支撑点。

4. 安全经济方法

由于安全的相对性原理，即在一定的经济技术条件下，安全目标是有限的。也就是说，安全系统的“优化”同样受制于经济。但是，由于安全经济的特殊性（安全性投入与生产性投入的渗透性、安全投入的超前性与安全效益的滞后性、安全效益评价指标的多目标性、安全经济投入与效用的有效性等），要求安全系统工程方法在考虑系统目标时要有超前的意识和方法，要有指标（目标）的多元化的表示方法和测算方法。

因此，应尽可能地做到以下两点：一是以一定的安全投入，取得最大的安全效益；二是在取得一定的安全效益时，使得安全投入最小。这就是通常所说的，以最小的安全投入取得最大的安全效益。安全投资效益的评价应该兼顾经济效益和社会效益，而这需要安全经济学理论和方法才能解决。

5. 系统安全管理方法

安全系统工程从学科的角度讲是自然科学与社会科学相交叉的横断学科，从系统科学原理的角度讲它是解决安全问题的一种科学方法，所以安全系统工程是理论与实践紧密结合的专业技术基础，系统安全管理方法则贯穿到安全的规划、设计、制造、使用、控制、检查的全过程。所以，系统安全管理方法是安全系统工程方法的重要组成部分。

第三节　安全系统工程的产生与发展

事故给人类带来无数灾难，严重地制约了经济发展和社会进步，甚至对人类生存构成巨大威胁。然而，事故的影响也并非都是消极的，首先，事故具有鲜明的反面教育的作用，它向人们展示了破坏的恶果，指导人们必须按照科学规律办事；其次，事故是一种特殊的科学实验，一个系统发生事故说明该系统存在不安全、不可靠问题，人们通过对事故的调查、分析、实验找出事故原因，研究并采取了有效控制事故的措施，改进系统工艺，完善设备，完善安全技术措施，从而提高系统的性能并发展专业技术，最后，事故是诞生新的科学技术的催化剂，事故的强大负面效应对人类产生巨大的冲击作用，激发人类以更大的决心和更大的力量研究事故。通过对事故信息及资料的收集、整理分析、模拟实验等，也就是充分开发利用“事故资源”，一个崭新的学科——安全系统工程就在人们这种不懈努力与坚苦卓绝的斗争中诞生了。在科学技术发展的历史长河中，许多学科的诞生都离不开事故这种反作用，离不开故障、失败带来的反作用。

安全系统工程产生于20世纪60年代初期美英等工业发达国家。这一时期，由于美国在导弹系统研发过程中仅仅一年半的时间就连续发生4起重大事故，损失惨重，从而迫使美国空军以系统工程的基本原理和管理方法来研究导弹系统的安全性、可靠性，并于1962